UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,028	12/11/2003	Blair B. Dillaway	MSFT-2795/305124.1	2338

41505 7590 09/11/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
09/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/734,028	DILLAWAY ET AL.	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **12-11-2003**.

2. Claims **1 - 30** are pending. Claim **1, 19** are independent.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim **1 - 14, 17 - 27, 29, 30** are rejected under 35 U.S.C. 102(e) as being anticipated by **Yan et al.** (US PGPUB No. **20050033987**).

Regarding Claims 1, Yan discloses a method of establishing trust between independent first and second computer-type entities, the first entity operating in a trusted manner on a computing device and seeking a trust-based relationship with the second entity, whereby the first entity constructs an attestation message to be delivered to the second entity, the attestation message including a code identifier (code ID) representative of the first entity and data relevant to the purpose of the trust-based relationship, the second entity having knowledge of each valid code ID corresponding to the first entity, the first entity appends a digital signature to the attestation message and

a certificate chain leading back to a trusted root authority, the signature being based on the code ID and data thereof and being verifiable based on a security key included in the certificate chain, the certificate chain including at least one certificate therein proffering trustworthiness of the computing device of the first entity, and the first entity sends the attestation message to the second entity and the second entity receives same, the method comprising:

a) the second entity verifying the signature of the received attestation message based on the included security key, whereby alteration of the code ID or data of the attestation message should cause the signature to fail to verify, the second entity based on such a failure dishonoring such attestation message; (see Yan paragraph [0058], lines 1-10; paragraph [0061], lines 12-16: attestation techniques utilized; paragraph [0060], lines 1-6: verify attestation message; paragraph [0060], lines 6-9; paragraph [0019], lines 10-13: modification of configuration data (attestation message information, certificate information revoked), attestation information dishonored)

b) the second entity deciding whether to in fact enter into the trust-based relationship with the first entity based on the code ID and the data in the attestation message; (see Yan paragraph [0060], lines 6-11: determination whether accept trust relationship)

c) the second entity upon deciding to in fact enter into the trust-based relationship with the first entity constructing a trust message to be delivered to the first entity, the trust message establishing the trust-based relationship and including therein

a secret to be shared between the first and second entities, where such shared secret allows such first and second entities to communicate in a secure manner; (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: secret (session key) exchanged for future messaging, communications) and

d) the second entity sending the trust message to the first entity and the first entity receiving same, whereby the first entity obtains the shared secret in the trust message and employs the shared secret to exchange information with the second entity according to the established trust-based relationship with such second entity. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session exchanged between entities, utilized for future messaging between entities)

Regarding Claims 2, Yan discloses the method of claim 1 wherein the first entity encrypts at least one of the code ID and the data of the attestation message according to a key available to the second entity, the method further comprising the second entity decrypting such encrypted matter. (see Yan paragraph [0059], lines 6-12: certificate (public/private) key available to second entity, utilized to encrypt (signature) attestation information)

Regarding Claims 3, Yan discloses the method of claim 1 wherein the second entity consumes the attestation message by application of same to a verifying function that automatically verifies the attestation message based on a format thereof and that

extracts relevant information from such verified attestation message for use by the second entity. (see Yan paragraph [0060], lines 6-9: verify attestation message with extracted information based on formatted information (certificate information, encrypted hash))

Regarding Claims 4, Yan discloses the method of claim 1 wherein the second entity decides based on the code ID of the first entity in the attestation message therefrom whether the second entity can be trusted, and also decide based on the certificate chain of the message whether the computing device can be trusted. (see Yan paragraph [0060], lines 9-12: entity can be trusted; paragraph [0060], lines 1-6: certificate chain utilized to establish trust)

Regarding Claims 5, Yan discloses the method of claim 4 wherein the second entity identifies the first entity based on the code ID thereof and decides based on the identity of the first entity whether such first entity can be trusted. (see Yan paragraph [0060], lines 6-9: integrity metric (code ID) of first entity utilized in trust determination)

Regarding Claims 6, Yan discloses the method of claim 5 wherein the second entity determines that the identified first entity is not on a do-not-trust list. (see Yan paragraph [0060], lines 6-9: check identity on certificate revoked list (do-not-trust list))

Regarding Claims 7, Yan discloses the method of claim 4 wherein the second entity

determines that the code ID is a known code ID and that the first entity can be trusted based on such code ID. (see Yan paragraph [0060], lines 6-9: check first entity on application trust list based on integrity metric (code ID) of first entity)

Regarding Claims 8, Yan discloses the method of claim 4 wherein the second entity determines from the certificate chain whether the computing device of the first entity should be trusted to instantiate and execute the first entity in a trusted manner and should be trusted to calculate the code ID properly. (see Yan paragraph [0060], lines 1-9: certificate information utilized to determine trust status)

Regarding Claims 9, Yan discloses the method of claim 8 wherein the second entity determines that each certificate in the certificate chain is not on a do-not-trust list. (see Yan paragraph [0060], lines 6-9: check certificate in certificate chain, not on revoked list (do-not-trust list))

Regarding Claims 10, Yan discloses the method of claim 1 wherein the second entity constructs a trust message including therein a shared secret comprising a symmetric key (K) that the first and second entities shall each employ to encrypt and decrypt messages therebetween. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging)

Regarding Claims 11, Yan discloses the method of claim 10 wherein the second entity

constructs a trust message including therein the symmetric key (K) encrypted according to a public key of the first entity (PU-1) to result in (PU-1(K)), the second entity obtaining (PU-1) from the certificate chain of the attestation message, and wherein the first entity obtains the symmetric key (K) from the received trust message by applying a private key (PR-1) corresponding to (PU-1) to (PU-1(K)) to result in (K). (see Yan paragraph [0059], lines 6-12: public/private certificate key, encrypt (signature) attestation information)

Regarding Claims 12, Yan discloses the method of claim 1 wherein the second entity constructs a trust message further including therein an identification of a cryptographic algorithm to be employed in connection with the shared secret. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key for secure communications (interaction); paragraph [0065], lines 9-15: updated attestation information (cryptographic algorithm), protocol for exchange negotiated)

Regarding Claims 13, Yan discloses the method of claim 1 wherein the second entity constructs a trust message further including therein the code ID of the first entity as obtained from the attestation message. (see Yan paragraph [0059], lines 6-12: generate (integrity metric (code ID), attestation information)

Regarding Claims 14, Yan discloses the method of claim 1 wherein the second entity constructs a trust message further including relevant trust data encrypted according to a

key available to the first entity, and wherein the first entity decrypts the encrypted trust data by applying the key thereto. (see Yan paragraph [0059], lines 6-12: public/private key certificate (available to first entity) used to encrypt (signature) attestation information)

Regarding Claims 17, Yan discloses the method of claim 1 whereby the trust message is a first trust message and the shared secret is a first shared secret, the method further comprising: the second entity constructing a second trust message to be delivered to the first entity, the second trust message including therein a second secret to be shared between the first and second entities, where such second shared secret allows such first and second entities to communicate in a secure manner; the second entity sending the second trust message to the first entity and the first entity receiving same, whereby the first entity obtains the second shared secret in the trust message and employs the second shared secret to exchange information with the second entity, the first shared secret no longer being valid. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future communications)

Regarding Claims 18, Yan discloses the method of claim 1 wherein prior to the first entity constructing the attestation message, the first entity sends a can-attest message to the second entity, the can-attest message stating that the first entity can send an attestation message but that the first entity would like to know from the second entity whether such an attestation message is required by such second entity and if so any

requirements that such second entity has with regard to such attestation message, the method further comprising the second entity sending an attestation-wanted message to the first entity in response to the can-attest message, the attestation-wanted message stating that the second entity does in fact require an attestation message from the first entity and that the attestation message as sent by the first entity must adhere to certain requirements as defined in such attestation-wanted message, whereby the first entity thereafter sends the attestation message in accordance with the requirements stated in the attestation-wanted message. (see Yan paragraph [0065], lines 9-15: update attestation (wanted-message) information, negotiate protocol for exchange of attestation information)

Regarding Claims 19, Yan discloses a method of establishing trust between independent first and second computer-type entities, the first entity operating in a trusted manner on a computing device and seeking a trust-based relationship with the second entity, the method comprising:

a) the first entity constructing an attestation message to be delivered to the second entity, the attestation message including a code identifier (code ID) representative of the first entity and data relevant to the purpose of the trust-based relationship, the second entity having knowledge of each valid code ID corresponding to the first entity (see Yan paragraph [0060], lines 6-9: check entity integrity metric (code ID), identify on application trust list);

b) the first entity appending a digital signature to the attestation message and a certificate chain leading back to a trusted root authority, the signature being based on the code ID and data thereof and being verifiable based on a security key included in the certificate chain, the certificate chain including at least one certificate therein proffering trustworthiness of the computing device of the first entity; (see Yan paragraph [0060], lines 1-6: certificate chain utilized for attestation information, (exchange, verification))

c) the first entity sending the attestation message to the second entity and the second entity receiving same, whereby the second entity verifies the signature of the received attestation message based on the included security key (see Yan paragraph [0060], lines 6-9: verify signature, attestation information), whereby alteration of the code ID or data of the attestation message should cause the signature to fail to verify, the second entity based on such a failure dishonoring such attestation message, the second entity decides whether to in fact enter into the trust-based relationship with the first entity based on the code ID and the data in the attestation message, the second entity upon deciding to in fact enter into the trust-based relationship with the first entity constructs a trust message to be delivered to the first entity, the trust message establishing the trust-based relationship and including therein a secret to be shared between the first and second entities, where such shared secret allows such first and second entities to communicate in a secure manner, and the second entity sends the trust message to the first entity and the first entity receiving same; (see Yan paragraph

[0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging, communications) and

d) the first entity obtaining the shared secret in the trust message and employing the shared secret to exchange information with the second entity according to the established trust-based relationship with such second entity. (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key exchanged between entities for future messaging, communications)

Regarding Claims 20, Yan discloses the method of claim 19 wherein the first entity constructs an attestation message including a code identifier (code ID) calculated from a digest of the first entity, whereby alteration of the first entity causes the code ID to change. (see Yan paragraph [0065], lines 9-15: updated integrity metric (code ID) modified, new attestation protocol required)

Regarding Claims 21, Yan discloses the method of claim 20 wherein the first entity constructs an attestation message including a code identifier (code ID) calculated from a digest of the first entity and from security information relating thereto, whereby alteration of the first entity or the security information causes the code ID to change. (see Yan paragraph [0065], lines 9-15: alteration of security information causes integrity metric (code ID) to be modified)

Regarding Claims 22, Yan discloses the method of claim 19 wherein the first entity

constructs an attestation message including trust information relevant to the trust-based relationship. (see Yan paragraph [0065], lines 9-15: generate attestation information with updated integrity information)

Regarding Claims 23, Yan discloses the method of claim 19 further comprising a code ID calculator on the computing device of the first entity calculating the code ID, the code ID calculator operating in a trusted manner on the computing device. (see Yan paragraph [0020], lines 7-8: generate integrity metric (code ID) on trusted device)

Regarding Claims 24, Yan discloses the method of claim 19 further comprising the first entity encrypting at least one of the code ID and the data of the attestation message according to a key available to the second entity, and the second entity decrypting such encrypted matter. (see Yan paragraph [0060], lines 1-9: public/private key certificate (know to second entity) utilized to encrypt (signature) attestation information, second entity must decrypt for verification)

Regarding Claims 25, Yan discloses the method of claim 19 wherein the first entity creates the attestation message by application of the code ID and data thereof to a quoting function that automatically produces the attestation message in an appropriate format that is accessible to the second entity. (see Yan paragraph [0065], lines 9-15: attestation information generated in an accessible format (negotiated) with second entity))

Regarding Claims 26, Yan discloses the method of claim 19 wherein the second entity constructs a trust message including therein a shared secret comprising a symmetric key (K) that the first and second entities shall each employ to encrypt and decrypt messages therebetween, the symmetric key (K) being encrypted according to a public key of the first entity (PU-1) to result in (PU-1(K)), the second entity obtaining (PU-1) from the certificate chain of the attestation message, the method comprising the first entity obtaining the symmetric key (K) from the received trust message by applying a private key (PR-1) corresponding to (PU-1) to (PU-1(K)) to result in (K). (see Yan paragraph [0062], lines 1-4; paragraph [0064], lines 1-4: session key utilized for messaging between first and second entities; paragraph [0059], lines 4-9: public/private key for encryption/decryption (signature attachment))

Regarding Claims 27, Yan discloses the method of claim 19 wherein the second entity constructs a trust message further including relevant trust data encrypted according to a key available to the first entity, the method comprising the first entity decrypting the encrypted trust data by applying the key thereto. (see Yan paragraph [0059], lines 6-12: attestation information encrypted (signature) based on public/private keys (known to first entity))

Regarding Claims 29, Yan discloses the method of claim 19 whereby the trust message is a first trust message and the shared secret is a first shared secret, and

whereby the second entity constructs a second trust message to be delivered to the first entity, the second trust message including therein a second secret to be shared between the first and second entities, where such second shared secret allows such first and second entities to communicate in a secure manner (see Yan paragraph [0062], lines 1-4; paragraph [0064] lines 1-4: session key exchanged between entities for future messaging), and the second entity sends the second trust message to the first entity and the first entity receives same, the method further comprising the first entity obtaining the second shared secret in the trust message and employing the second shared secret to exchange information with the second entity, whereby the first shared secret is no longer valid. (see Yan paragraph [0065], lines 9-15: update attestation information, previous attestation information invalid)

Regarding Claims 30, Yan discloses the method of claim 19 further comprising, prior to the first entity constructing the attestation message, the first entity sending a can-attest message to the second entity, the can-attest message stating that the first entity can send an attestation message but that the first entity would like to know from the second entity whether such an attestation message is required by such second entity and if so any requirements that such second entity has with regard to such attestation message, whereby the second entity sends an attestation-wanted message to the first entity in response to the can-attest message, the attestation-wanted message stating that the second entity does in fact require an attestation message from the first entity and that the attestation message as sent by the first entity must adhere to certain requirements

as defined in such attestation-wanted message, the first entity thereafter sending the attestation message in accordance with the requirements stated in the attestation-wanted message. (see Yan paragraph [0065], lines 9-15: attestation information (wanted-message) formatted in a negotiated format)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim **15** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Yan** in view of **Qui** (US PGPUB No. **20040148505**).

Regarding Claims 15, Yan discloses the method of claim 1 wherein the second entity constructs a trust message after which the shared secret and the established trust-based relationship are no longer valid. (see Yan paragraph [0060], lines 6-9: certificate revoked, trust relationship not valid if certificate revoked) Yan does not specifically disclose whereby an expiration time. However, Qui discloses wherein an expiration time. (see Qui paragraph [0040], lines 1-7; paragraph [0021], lines 8-11: expiration timer for certificate information)

It would have been obvious to one of ordinary skill in the art to modify Yan as taught by Qui to enable the capability for a trust message further including an expiration

time. One of ordinary skill in the art would have been motivated to employ the teachings of Qui in order to enable the capability for the generation, transmission, and updating of certificate information when the number of devices is large (see Qui paragraph [0007], lines 7-12: " ... *However, the generation, transmission and updating of certificates in association with hardware devices (i.e., the hardware devices are each associated with a certificate) may introduce problems in certificate management, transmission, control, use, etc., especially where the number of devices is large. ...* ")

7. Claims **16, 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yan** in view of **Grawrock** (US PGPUB No. **20040117625**).

Regarding Claims 16, Yan discloses the method of claim 1 wherein the second entity creates the trust message by application of the shared secret and other relevant information that automatically produces the trust message in an appropriate format that is accessible to the first entity. (see Yan paragraph [0059], lines 6-12: generate formatted attestation information) Yan does not specifically disclose whereby a sealing function. However, Grawrock discloses wherein a sealing function. (see Grawrock paragraph [0018], lines 12-16; paragraph [0025], lines 1-7; paragraph [0026], lines 1-6: seal/unseal trusted operation utilized)

It would have been obvious to one of ordinary skill in the art to modify Yan as taught by Grawrock to enable the capability to perform a seal operation within a trusted computing environment. One of ordinary skill in the art would have been motivated to

employ the teachings of Grawrock in order to enable the capability to enable local users and remote computing devices an efficient and easier method for the completion of trusted operations. (see Grawrock paragraph [0002], lines 7-14: " *... However, a local user of the platform may also want to establish a similar level of trust with the local platform or computing device. It is impractical, however, for a local user to perform the same complex calculations and participate in the same complex protocols with the fixed token as the remote computing devices in order to establish trust in the computing device. ...* ")

Regarding Claims 28, Yan discloses the method of claim 19 wherein the first entity consumes the trust message by application of same that automatically extracts the shared secret and other relevant information from such trust attestation message for use by the first entity. (see Yan paragraph [0060], lines 6-9: extracts attestation information for processing) Yan does not specifically disclose whereby an unsealing function. However, Grawrock discloses wherein an unsealing function. (see Grawrock paragraph [0018], lines 12-16; paragraph [0025], lines 1-7; paragraph [0026], lines 1-6: seal/unseal trusted operation utilized)

It would have been obvious to one of ordinary skill in the art to modify Yan as taught by Grawrock to enable the capability to perform an unseal operation within a trusted computing environment. One of ordinary skill in the art would have been motivated to employ the teachings of Grawrock in order to enable the capability to

enable local users and remote computing devices an efficient and easier method for the completion of trusted operations. (see Grawrock paragraph [0002], lines 7-14)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

C.J.

CVJ
August 20, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/4/07